REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-6, 8-15, 17-20, and 22-25 are pending in the application. The Examiner additionally stated that claims 1-6, 8-15, 17-20, and 22-25 are rejected. By this communication, claims 1, 6, 8, 17, 20, and 22-23 are amended. Hence, claims 1-6, 8-15, 17-20, and 22-25 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Claim Objections

The Examiner objected to claim 1 because it recites "a x86-compatible microprocessor" rather than "an 86-compatible microprocessor" and required appropriate correction. By this communication claim 1 is amended to properly recite the claimed element and it is requested that the objection to claim 1 be withdrawn.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-6, 8-15, 17-20, and 22-25 under 35 U.S.C. 103(a) as being unpatentable over Kessler et al. (US 6,789,147), hereinafter, "Kessler," in view of Juffa. (US 6,247,117), hereinafter, "Juffa." Applicant respectfully traverses the Examiner's rejections.

As per claims 1, 17, and 22, the Examiner noted that Kessler discloses an apparatus for performing cryptographic operations, comprising:

- an instruction register within a microprocessor (Fig. 1, item 10) having a cryptographic instruction disposed therein, wherein said cryptographic instruction is arranged according to the instruction format for execution on said x86-compatible microprocessor (col. 3, lines 40-45), and wherein said cryptographic

instruction is part of an application program, and wherein said x86-compatible microprocessor executes said application program, and wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a user-generated key schedule be employed for execution of said one of the cryptographic operations (noting that the execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue, and that the operation blocks correspond to cryptographic algorithms such as AES, 3DES, DES, and RC4) (column 9, lines 8-42; Fig. 8);

- a keygen unit, operatively coupled to said instruction register, configured to direct said x86-compatiblemicroprocessor to load said user-generated key schedule (column 12, lines 7-40); and
- an execution unit, operatively coupled to said keygen unit, configured to employ said user-generated key schedule to execute said one of the cryptographic operations (column 9, lines 7-43), said execution unit comprising:
    - a cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit (noting that the primitive security operation blocks include an Advanced Encryption Standard (AES) block 807, a Triple Data Encryption Standard (3DES) block 809, a modular exponentiation block 811, a hash block 813, a simple arithmetic and logic block 815, and an alleged RC4.RTM. block 819) (column 9, lines 8-22).

The Examiner conceded that Kessler does not explicitly specify wherein said cryptographic instruction is part of an application program, and wherein said microprocessor executes said application program, but that Juffa discloses an apparatus and method, which further disclose wherein said cryptographic instruction is part of an

application program, and wherein said x86-compatible microprocessor executes said application program (col. 8, lines 1-5; col. 17, lines 30-45; col. 23, lines 3-8; Fig. 11, items 10 and 404).

The Examiner thus concluded that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Kessler such as to use the x86-compatible microprocessor to execute the actual application program, noting that the motivation for doing so would have been in order to detect special and exceptional cases of defined data format in advantageous as taught by Juffa (col. 2, lines 55-65).

By this communication, Applicant has amended claims 1, 17, and 22 to recite, among other elements and limitations, a "single, atomic hash instruction," which, as one skilled in the art will appreciate, operates transparently in the presence of interrupts, as are commonly encountered when a general purpose microprocessor, such as an x86-compatible microprocessor, is executing any one of the application programs that are designed to be executed on an x86 microprocessor, such as Microsoft WindowsXP and Microsoft Outlook, as is taught in the instant specification.

The independent claims also recite "an x86-compatible microprocessor." By way of summary, the specification teaches that in order for any device to be deemed equivalent to an x86-compatible microprocessor as defined above, it must be 1) compatible with the x86 architecture, 2) it must include an x86 integer unit, 3) it must include an x86 floating point unit, 4) it must include an x86 MMX unit, and 5) it must include an x86 SSE unit. In addition, an equivalent device must 6) correctly execute a majority of the application programs that are designed to be executed on an x86 microprocessor.

Applicant has thoroughly studied the teachings of Kessler and Juffa, both alone and in combination, and finds that Kessler fails to teach any form of an x86-compatible microprocessor. As has been previously submitted, Kessler teaches a security co-processor interface. He does not teach an x86 integer unit, x86 floating point unit, x86 MMX unit, or x86 SSE unit. Kessler fails to teach or suggest the capability to correctly

execute a majority of the application programs that are designed to be executed on an x86 microprocessor.

Regarding the Examiner's statement that Juffa discloses an apparatus and method, which further disclose wherein said cryptographic instruction is part of an application program, and wherein said x86-compatible microprocessor executes said application program, Applicant respectfully responds that Juffa is entirely silent with regard to a single, atomic cryptographic instruction. Applicant has searched Juffa for any suggestion, allusion to, or even a hint regarding any form of cryptographic instruction and finds that Juffa utterly fails to teach this aspect of the present invention. Rather, Juffa teaches embedding a *microinstruction* in a microcode stream (that is, microcode generated by the processor itself to perform the suboperations required to execute a programmed *macro instruction* within an application program), where the microinstruction is directed towards detection of special and exceptional cases of floating point data that is provided along with a floating point macro instruction in an application program. This is all that Juffa teaches. He does not teach suggest, or allude to a single, atomic cryptographic instruction that is part of an application program executed by an x86-compatible microprocessor.

By combining the references, one skilled in the art would be led to conclude that the coprocessor of Kessler may be useful in an x86 environment because it could offload cryptographic functions which would otherwise have to be performed via operating system intensive subroutine calls. That is, one skilled would appreciate that the coprocessor of Kessler could be used to offload the x86-compatible microprocessor of Juffa for the performance of security functions.

As one skilled in the art will appreciate, an x86-compatible microprocessor is a general purpose microprocessor that is configured to execution commonly used application programs such as Microsoft WindowsXP and Microsoft Outlook. These two applications are specifically noted in the instant specification. And as one skilled will agree, both of these applications comprise provisions to interrupt the microprocessor as well as program control transfer instructions (e.g., JMP). Yet, Kessler specifically teaches away from employing a general purpose microprocessor, in that he asserts:

> Performing tasks to establish a secure session is processor intensive. If a general purpose microprocessor, acting as a host processor for a network element, performs these tasks, then the network element's system performance will suffer because resources will be consumed for the tasks. (col. 1, lines 56-61)

If the security operations taught by Kessler were to be performed by a host processor, it would thus defeat his stated purpose, which is to offload tasks from the host processor. (col. 1, line 66 – col. 2, line 39).

As is pointed out in the instant specification, message encryption and decryption are very commonly employed operations, and there has been a noted desire in the community to accelerate these operations because they have heretofore been performed via either dedicated calls to software subroutines or by co-processors such as that taught by Kessler. And there are numerous manufacturers of x86-compatible microprocessors to include Intel Corporation and Advance Micro Devices. Yet, *none* of these manufacturers have been able—to date—to develop an x86-compatible microprocessor that meets the elements and limitations recited in claims 1, 17, and 22. Accordingly, it is respectfully asserted that one of ordinary skill in the art at the time of the invention would have not been informed by the combination of Kessler and Juffa to yield the elements and limitations of the independent claims.

In addition to the above showings, Applicant respectfully notes that the combination of Kessler and Juffa fails to teach or suggest a "single atomic hash instruction" for execution on an "x86-compatible microprocessor." Applicant has searched all of the references to determine if there is any teaching, or practical motivation provided that would even allude to a single atomic cryptographic instruction. There is none. The references utterly fail to teach this limitation.

Again, regarding the combined teaching of the cited references, Applicant fails to understand how they could be combined in any practical manner to yield the elements and limitations recited in claim 1. That is, Kessler explicitly teaches that a security operation *cannot* be performed by a general purpose microprocessor (i.e., host processor)

and must be offloaded to a coprocessor—*a technique which is highlighted in the background of the instant specification as being limiting and disadvantageous*. Juffa essentially adds nothing other than translation of macro instructions into a microcode stream for execution on an x86-compatible microprocessor should benefit from the inclusion of a special checking microinstruction in the event that a floating point macro instruction is executed.

Again, none of the cited references teach a cryptography unit disposed in an x86-compatible microprocessor.

The references in combination doe not teach an x86-compatible microprocessor, nor does the combination teach a single, atomic cryptographic instruction (i.e., a macro instruction) within an application program that directs an x86-compatible microprocessor to perform a cryptographic operation. This is because, prior to the advent of the present invention, x86-compatible microprocessors could not be programmed via a single instruction to execute a cryptographic operation. There was no instruction, nor was there a cryptographic unit therein capable of performing the operation.

It is thus respectfully submitted that the combination of Kessler and Juffa does not contemplate or suggest an x86-compatible microprocessor that includes a cryptographic unit within its execution stage. Hence, it further does not follow that the references, in combination would suggest a single, atomic cryptographic instruction which is part of an application program being executed by the x86-compatible microprocessor, and which directs that the microprocessor perform a cryptographic operation. It is respectfully submitted that any microprocessor that lacks a cryptographic unit therein would be incapable of performing the cryptographic function directed by the single, atomic cryptographic instruction. A skilled artisan would be forced to employ the technique taught by Kessler (i.e., offload the hash to a coprocessor) or the software technique taught by other references (i.e., execute hundreds of macroinstructions ("software modules") to perform the operation on a general purpose microprocessor—both techniques of which are shown to be inferior to the present invention.

Accordingly, it is requested that the rejections of claims 1, 17, and 22 be withdrawn.

With respect to claims 2-6 and 8-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler and Juffa. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6 and 8-15.

With respect to claims 18-20, these claims depend from claim 17 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler and Juffa. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 18-20.

Claims 23-25 depend from claim 22 and add further limitations that are neither anticipated nor made obvious by the combination of Kessler and Juffa. Accordingly, Applicant respectfully submits that claims 23-25 are allowable as well.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-6, 8-15, 17-20, and 22-25 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

05/02/2009

Date: _____